Goals

- Review recent data breaches
- Highlight lessons learned
  - 9 patterns of attacks
- Best practices

Recent Data Breaches

- **Verizon** – 1,500,000 records exposed on 3/24/16
- **21st Century Oncology** – 2,200,000 records exposed, a hacker gained access to a patient database
- **Centene** – 950,000 records exposed because of 6 missing hard drives with PHI
- **JP Morgan** - 76 million households and 7 million small businesses
  
  Easy to share large volumes of data!

Recent Data Breaches – Healthcare

- Aventura Hospital and Medical Center – an employee improperly accessed 82,601 patient records
- Central Utah Clinic – notifying 30,000+ patients of a potential data breach after discovering hacker’s had accessed on of the clinic’s servers
- Duke University Health System – notified patients due to a stolen thumb drive that contained unencrypted patient names and physician names
- Memorial Hermann Health Systems – notifying 10,000+ of a security breach due to an employee accessing unauthorized patient information
- St. Elizabeth’s Medical Center – notified patients of a potential data breach after a laptop and thumb drive were stolen from a physician’s home
- Cedars-Sinai Medical Center in Los Angeles – notified 500+ patients that their protected health information may have been compromised due to an unencrypted laptop being stolen from an employee’s home
- Beth Israel Deaconess Medical Center to pay $1100K to settle data breach
Recent Data Breaches – Small #, Big Impact

- In 2015, there were 255 data breaches affecting 500 or more individuals reported to HHS Office of Civil Rights, and these breaches affected a total of more than 112 million health records.
- With the United States population at ~322.8 million, ~34.7 percent of the population’s health records were compromised last year.
- The three biggest healthcare data breaches of all time were reported in 2015, and the five biggest breaches of the year including the cyberattacks on Indianapolis-based Anthem and Mountaintake Terrace, Wash.-based Premera Blue Cross — alone affected 108.2 million individuals.

Recent Data Breaches – Other HC Notes

- Out of the 90,000+ HIPAA breach cases OCR has received since 2003 – 17% have resulted in fines.
- HHS Office for Civil Rights Director indicates that most HIPAA-covered entities fail to perform a comprehensive, thorough risk analysis and fail to apply the results of that analysis.

Recent Data Breaches – General Costs

- Lost customers and reputation—$$ to replace
- Ponemon Institute - $201/breached record**
  - 20% probability of 10,000 record breach in HC
- The forecasted average for 1,000 records is between $52,000 and $87,000***
- Juniper Networks - $2.1 Trillion by 2019*

Recent Data Breaches – Cost Components

- Immediate Response Activities
  - Conduct investigation/forensics to determine root cause
  - Determine probable victims
  - Organize Incident Response team
  - Prepare notification and disclosure documents for victims and regulatory authorities
  - Ramping up call center
- Aftermath Activities
  - Audit and consulting services
  - Legal services for defense and compliance
  - Free or discounted services to victims
  - Identity theft protection services
  - Lost customer business or customer churn

Recent Data Breaches – OCR Penalties

- New York and Presbyterian Hospital agreed to pay OCR $3,300,000 to settle potential violations by failing to secure thousands of patient’s electronic protected health information (ePHI) held on their network. Columbia University paid $1,500,000 for their part in the joint breach.
- Parkview Health System has agreed to pay $800,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program in medical records dumping case.
- Concentra Health Services agreed to pay $1,725,220 to settle potential violations after unencrypted laptop was stolen from one of its facilities. Concentra had taken steps to begin encryption but the efforts were incomplete and inconsistent over time.

Recent Data Breaches – Health Hazards

- ECRI 2015 Top 10 Health Technology Hazards

2. Data integrity: Incorrect or missing data in electronic health records and other health IT systems

9. Cybersecurity: Insufficient protections for medical devices and systems
Recent Data Breaches - Target

• Target
  – On December 19, 2013, Target publicly confirmed that 40 million credit and debit card accounts were exposed in a breach of its network.
  – Thieves were able to sell information from these cards via online black market forums known as “card shops.”
  – The websites list card information including the card type, expiration date, track data (magnetic stripe), country of origin, issuing bank, and successful use rate.
  – Malware new variant of “BlackPOS” (a.k.a. “Kaptoxa”) designed to steal data from cards when swiped at infected point-of-sale systems running Microsoft Windows.

Recent Data Breaches – Physical Impact

• Cyber Attack Caused Damage at German Steel Mill
  (January 8, 2016)

  A cyber attack on a German steel mill caused damage to the facility. The attackers disrupted the plant’s control system to make it impossible to shut down a blast furnace properly. The damage was described as “massive”. This is the second documented case of a cyber attack causing physical damage – the first was Stuxnet.

• Polish Airlines LOT System Delayed Flights by DoS attack on ground computer systems.

How do hackers and fraudsters break in?

• Social Engineering

• Email Phishing
  – “Spear Phishing”

• Remote Access

• Third-Party

The Fine Art of “People Hacking”

• Social Engineering uses non-technical attacks to gain information or access to technical systems:
  – Pre-text telephone calls:
    “Hi, this is Randy from Comcast. I am working with Mike, and I need your help…”
  – Building penetration:
    ◦ Seeding
      ◦ Email attacks
**Physical (Facility) Security**

Compromise the site:

- "Hi, Joe said he would let you know I was coming to fix the printers..."

Plant devices:

- Keystroke loggers
- Wireless access point
- Thumb drives ("Switch Blade")

**Phishing attacks**

- Phishing heavily used in espionage attacks – targeting executives – “inevitability of the click” – 3 e-mails to get a click!!
- ‘Ands’ –
  - User needs to take action and
  - Need a vulnerability and
  - Software needs to be quietly installed and
  - Needs a communication path back to attacker

**Spear Phishing**

“Second Generation” phishing

Goal is to “root the network”

Install malware

- Log system activity to harvest passwords
- Use automated tools to execute fraudulent payments

Trick Administrative system users or Executives into supplying privileged userids and passwords

**3 Primary Motives for Attacks**

- Financial Gain – Organized-crime/worldwide
- Espionage/Intellectual Property (IP) – China
- Hacktivism/activism

**TrustWave – Intrusion Analysis Report**

Top Methods of Entry Included:

- Remote Access Applications (45%)
- Default vendor supplied or weak passwords (39%)
- 3rd Party Connections (42%)
  - MPLS, ATM, Frame Relay
- SQL injection (9%) – Web application compromises (30%)
- Exposed Services (4%)

**Verizon Data Breach Investigation Report (DBIR) 2013**

- Spear Phishing – “Second Generation” phishing
  - Goal is to “root the network”
  - Install malware
    - Log system activity to harvest passwords
    - Use automated tools to execute fraudulent payments
  - Trick Administrative system users or Executives into supplying privileged userids and passwords

- Physical (Facility) Security
  - Compromise the site:
    - "Hi, Joe said he would let you know I was coming to fix the printers..."
  - Plant devices:
    - Keystroke loggers
    - Wireless access point
    - Thumb drives ("Switch Blade")

- Phishing attacks
  - Phishing heavily used in espionage attacks – targeting executives – “inevitability of the click” – 3 e-mails to get a click!!
  - ‘Ands’ –
    - User needs to take action and
    - Need a vulnerability and
    - Software needs to be quietly installed and
    - Needs a communication path back to attacker

- Spear Phishing
  - “Second Generation” phishing
  - Goal is to “root the network”
  - Install malware
    - Log system activity to harvest passwords
    - Use automated tools to execute fraudulent payments
  - Trick Administrative system users or Executives into supplying privileged userids and passwords

- Primary Motives for Attacks
  - Financial Gain – Organized-crime/worldwide
  - Espionage/Intellectual Property (IP) – China
  - Hacktivism/activism

- TrustWave – Intrusion Analysis Report
  - Top Methods of Entry Included:
    - Remote Access Applications (45%)
    - Default vendor supplied or weak passwords (39%)
    - 3rd Party Connections (42%)
      - MPLS, ATM, Frame Relay
    - SQL injection (9%) – Web application compromises (30%)
    - Exposed Services (4%)
**NIST Authentication Factors**

- Single-Factor Authentication – something you know - password
- Two-Factor Authentication – something you physically have (i.e., a secure ID token or cell phone for Phone Factor authentication)
- Three-Factor Authentication – something you are – biometric authentication (retina, palm veins)

"2 Factor is any 2 of the above"

**9 Key Patterns of Attacks**

- Point-of-sale (POS) Intrusions
- Crimeware
- Cyber espionage
- Insider misuse
- Web app attacks
- Misc. errors
- Physical theft/loss
- Card skimmers
- DoS attacks

**9 Key Patterns of Attacks related to HC**

- Miscellaneous errors 32%
- Insider misuse 26%
- Physical theft/loss 16%
- Point-of-sale intrusion 12%
- Web app attack 9%

Frequency of data disclosures by incident patterns and victim industry

**Lessons Learned – Boston Children’s Hospital**

In reflecting on the Anonymous attack, the BCH CIO noted:

- Distributed Denial of Service (DDoS) countermeasures are crucial. BCH shut down all web-sites and e-mail. Staff communicated using a secure text messaging application the hospital had recently deployed
- Know which systems depend on external Internet access. In BCH’s event, the EHR system was spared, but the e-prescribing system wasn’t
- Make no excuses when pushing security initiatives. Children’s had to shut down email, e-prescribing and external-facing websites quickly
- Separate signals from noise
Overall Approach - TK²

- Train your people - Users and Executives who are knowledgeable and savvy
- Know your network –
  - Make your networks resistant to malware
  - Segment your network
  - Make it visible to Executive management
- Know your data - data first approach
  - minimum necessary access – know access paths

Ten Keys to Mitigate Risks

1. Strong policies and training – e-mail use, strong password requirements
2. Defined user roles and permissions – minimum necessary
3. Hardened internal systems – change default passwords, media limitations (CD, USB devices), disallow local admin rights on workstations
4. Encryption strategy – mobile
5. Vulnerability management process – patch and test
6. Well defined perimeter security layers: "Know Your Network“ and audit your third-party technology service providers
7. Data classification strategies “Know Your Data”
8. Defined incident response plan and procedures
9. Centralized audit logging, analysis, and automated alerting capabilities
10. Test, Test, Test

Questions?

Hang on, it’s going to be a wild ride!!

Juli Ochs, Health Care Director
CliftonLarsonAllen
juli.ochs@claconnect.com
(612)397-3011

Lee Painter, Manager
CliftonLarsonAllen
lee.painter@claconnect.com
(309) 202-9531